Research and Recommendations
Online Threat Monitoring for ORGANIZATION

Summary

Key personnel at ORGANIZATION have expressed concerns about harassment and other threats emerging online. This article from Mother Jones was specifically cited as a type of threat for which ORGANIZATION would like to have monitoring and notification in place in the event that ORGANIZATION or its personnel are named in forums or other online communities such as referenced in the article.

A preliminary round of research taking approximately two (2) hours failed to identify any obvious services that could meet this need. In fact, an online discussion on the active NTEN community revealed specific gaps in this space for social justice organizations.

In discussion with CONTACT, we agreed to provide a small scope of work (this proposal) to spend more time conducting research and evaluating the landscape of such services in more detail

About Online Threat Monitoring Services

This was a difficult task to perform. Having already invested two hours in researching and reaching out to colleagues prior to this project starting, I had failed to identify a single candidate for these services. After an additional two hours I had still failed to find any promising candidates. One of the challenges are that there are not standard naming conventions for the desired service(s). Below are just some of the terms I encountered and search working identify the services desired by ORGANIZATION:

Dark Web Monitoring
Deep/Dark Web Monitoring
Social Media Monitoring
Online Threat Monitoring
Corporate Brand Monitoring
VIP Protection
Corporate Protection
Attack Vector Visibility
Threat Monitoring
Threat Intelligence

Other challenges I encountered are that these services are not a standardized offering and services in this general space can be offered by cybersecurity firms, corporate security firms, intelligence analyst consultancies and more. Pricing is difficult to obtain and "apples to apples" comparisons between services and providers is difficult at best.

Approach

The approach I took was to first reach out to a broad network of colleagues I have developed over many years of work in the nonprofit technology, cybersecurity and digital privacy space. Out of my entire network of dozens of cybersecurity and nonprofit technology professionals, I only got one name. Concentric. They came recommended specifically by an organization who litigates against white nationalists and other hate groups. I was able to get a conversation with one of Concentric' intelligence analysts and I have a proposal from them for ORGANIZATION.

Using other platforms such as G2.com and Owler I managed to find an additional dozen or so providers that offered services in this field. I was able to eliminate most as candidates due to them being clearly focused on cybersecurity threat monitoring and/or being clearly focused on corporate and VIP protection for large enterprises.

Selection Process

It was difficult to impossible to get pricing estimates for any of these services without engagement in a demo or sales conversation. Given the time constraints on the project, I could not engage with more than three (3) vendors. I selected the three that seemed to be the best fit for ORGANIZATION's needs based on review of their websites, services and target market. These were:

1) Concentric
2) DigitalStakeout
3) LifeRaft Navigator

Challenges for ORGANIZATION

To this point, I cannot recommend any of these services to ORGANIZATION without reservation. Here are the challenges, from my perspective:

DigitalStakeout and LifeRaft's Navigator are vastly more affordable choices (between $9,000 and $15,000 annually. However, both will require either a ORGANIZATION personnel to learn and manage the platform and intelligence generated OR for ORGANIZATION to engage a third party to perform that work them.

Concentric provides more of a "done for you" approach where they compile and analyze the intelligence provided by these platforms into digestible reports for you, but this comes at a premium cost of $78,000 annually, 5-8 times more expensive than DigitalStakeout or LifeRaft Navigator.

Recommendations

Based on this research, if I had to choose a platform for ORGANIZATION, I would select DigitalStakeout. Again, this recommendation is not without significant reservations. While DigitalStakeout is the most cost-effective solution I was able to find, it will require significant investment of additional resources from ORGANIZATION to either:

- Train in-house staff to use the DigitalStakeout platform and provide threat intelligence to ORGANIZATION
- Engage an outside consultant/3rd party to manage the DigitalStakeout platform for ORGANIZATION and provide this intelligence.

Update - November 27, 2019

I followed up with DigitalStakeout to ask more specific questions about time and skills requirement to leverage their platform to meet ORGANIZATION's requirements. Responses below. I have found DigitalStakeout to be highly responsive and friendly throughout the inquiry process.

1. **What skills/experience does the designated analyst need in order to effectively use the platform?**

Anyone with a general understanding of web/it/security/social technologies (from websites to social media) can be trained to use the solution. The person administering social media or the website would be the most logical fit. Training will be provided by DigitalStakeout, and we have searchable online documentation for ongoing questions.

2. **How much time should the designed analyst plan on spending in the first month of using DigitalStakeout?**
   Training will be 30 min-1hr, plus we would recommend a monthly follow-up call during the first month to align feeds for the organization. As part of the training, we will assist the designated analyst set-up the needed monitors & alerts. Customers are more than welcome to engage support to get settled and confident in using features & tools in the platform.
3. **How much time per month should the designated analyst plan on spending to manage and analyze threats for their organization?**
   The DigitalStakeout solution is alert based. Usage time will depend on the number of alerts surfaced in a month. Budget to use the platform approximately 30mins – 1hr a week to review results and alerts.
4. **What level of support does DigitalStakeout provide for escalated threat analysis?**
   DigitalStakeout has a Support team whose function is to assist customers with inquiries about how to use our solution. The support and knowledge base should enable the end-user to perform common incident tasks such as a social media abuse claim.
   If a threat arises to a level of major concern, the customer should escalate the discovery to the organization's legal or law-enforcement channels. If the organization needs support through these incidents, we can recommend third-party vendors that can contract with the customer directly for support.
5. **Are there additional costs associated with the escalations?**
   The use of DigitalStakeout products do not entail incremental fees and costs would be handled directly with the third-party vendor.

Pricing

DigitalStakeout is $9,000 for a one-year contract for access to their threat intelligence platform. LifeRaft is $14,500 for a one-year contract for access to their threat intelligence platform. Concentric is $78,000 per year for Intelligence Monitoring and Threat Management for up to ten (10) items. For pricing purposes, an “item” would be a name, organization or other nameable asset to monitor.

Next Steps

I am not confident that this scope of work was sufficient to gain a thorough perspective on the landscape of these services. I still think it is possible that there are more cost-effective and appropriate solutions to meet this need for ORGANIZATION, but at this point I have been unable to identify any better options than the ones presented here. One decision point for ORGANIZATION is whether to make a decision from this information (e.g. “satisfice”) or continue investigating or consider drafting an RFP.